Feasibility of free space quantum key distribution with coherent polarization states

D Elser[1,2]**, T Bartley**[1,3]**, B Heim**[1,2]**, Ch Wittmann**[1,2]**,
D Sych**[1,2] **and G Leuchs**[1,2]

[1] Institute of Optics, Information and Photonics, University of Erlangen-Nuremberg, Staudtstr. 7/B2, 91058 Erlangen, Germany
[2] Max Planck Institute for the Science of Light, Günther-Scharowsky-Str. 1, Building 24, 91058 Erlangen, Germany
[3] Physics Department, Blackett Laboratory, Imperial College, London SW7 2BZ, United Kingdom

E-mail: `Dominique.Elser@mpl.mpg.de`

Abstract. We demonstrate for the first time the feasibility of free space quantum key distribution with continuous variables under real atmospheric conditions. More specifically, we transmit coherent polarization states over a 100 m free space channel on the roof of our institute's building. In our scheme, signal and local oscillator are combined in a single spatial mode which auto-compensates atmospheric fluctuations and results in an excellent interference. Furthermore, the local oscillator acts as spatial and spectral filter thus allowing unrestrained daylight operation.

1. Introduction

Quantum key distribution (QKD) [1, 2] is the process of establishing a secret shared key between two parties, traditionally named Alice and Bob. The security is based on the laws of quantum mechanics, in contrast to classical schemes, where security relies on the unproven lack of efficient mathematical algorithms. A QKD system typically comprises a quantum channel and an authenticated classical channel. Alice and Bob initially exchange quantum states over the quantum channel which might be completely under the control of an eavesdropper (called Eve). In a second step, Alice and Bob use the classical channel to distil a secret key from measurement results taken during the first step. Eve may listen to this classical information but not modify it. In our experiment, we focus on the first step, more precisely on the generation, transmission and measurement of coherent polarization states providing the raw data for QKD. Our main focus is on the characterization of a real-world free space channel with regard to continuous-variable QKD.

1.1. Free space quantum communication

In classical telecommunication, free space optics (FSO) [3] can help to solve the "last mile" problem: connecting end users to network nodes where installing optical fibres is often prohibitively time-consuming and expensive. Furthermore, FSO is utilized for satellite-to-ground and inter-satellite communication. In the domain of QKD, FSO offers an additional benefit: since fibre losses limit the maximum link range‡, FSO via satellite relays is currently the only feasible way to accomplish QKD over large distances.

The first demonstration of free space QKD over an atmospheric channel outside the laboratory was performed in 1996 [4]. Since then, several prepare-and-measure [5, 6, 7, 8, 9] and entanglement-based [10, 11, 12, 13] systems have been implemented. Currently, the world record distance is 144 km [9, 11] and satellite QKD is in the early phases of development [14, 15]. A common feature of all aforementioned systems is the use of single-photon detectors which, however, are impaired already by low background light intensities. Background light might stem from natural sources like the sun or the moon as well as from artificial illuminants such as street lamps [5]. In order to reduce this background noise, temporal, spectral and/or spatial filtering is employed [16]. Despite this, performance in daylight is still degraded compared to night operation [7].

In our system, we use an alternative approach: with the help of a bright local oscillator (LO) we perform homodyne measurements on weak coherent states. The primary task of the LO is to make the weak signal detectable by standard PIN photodiodes. Interestingly, apart from enabling homodyne measurements, the LO fulfils additional functions in our free space system:

Spatial filtering: Only photons which are spatially mode-matched to the LO produce a significant signal on the detector. The LO thus acts as a perfect single-mode spatial filter. Additional filtering (e.g. by pinholes or glass fibres) as used in single photon experiments is not required.

Spectral filtering: Our detection bandwidth can be precisely adjusted by electronic filtering of the homodyne signal. Background light outside this bandwidth does not perturb the measurement. Interference filters, commonly used in single photon experiments, exhibit orders of magnitude larger bandwidths and are lossy [16]. Atomic filters [17] perform better but still add complexity to the experiment.

Spatial tracking: In our setup, the LO propagates in the same spatial mode as the signal. Thus spatial beam jitter and distortions can easily be monitored in order to compensate for them; no additional beacon beam is needed.

Timing generation: Atmospherically induced time jitter can be determined from a pulsed LO. Thus the LO could fulfil the same task as the timing pulses in e.g. [7].

For a homodyne detection, a good interference of signal and LO is crucial. Stabilizing this interference would be a problem if, as usual, signal and LO were propagating as two separate beams. In our setup, however, we use polarization states which allow for co-propagation of signal and LO in one single beam (see section 1.3). Thus the interference is intrinsically excellent which results in a high detection efficiency. Furthermore, phase fluctuations in the channel are auto-compensated.

‡ This limitation could be overcome by using quantum repeaters which, however, are not yet available.

1.2. Continuous-variable quantum key distribution

The well-known BB84 protocol [18] makes use of the non-orthogonality of single-photon polarization states (*discrete variable*). The implementations of BB84, however, mostly approximate single photons by attenuated coherent states which can be conveniently produced. In 1992, Bennett realized that, due to their inherent non-orthogonality, coherent states (*continuous variable*) can be directly used for QKD [19]. In the original B92 protocol, the detection was still performed by discrete single photon detectors. Later, continuous-variable protocols also using continuous homodyne detection were proposed [20]. PIN photodiodes used in homodyne detectors offer higher quantum efficiencies than single-photon avalanche photodiodes.

In homodyne QKD systems, signal and local oscillator (LO) typically propagate in the same channel. Hence the bright LO has to be multiplexed with the signal which otherwise would be masked. In fibre-based experiments, temporal multiplexing by pulsing the LO [21, 22, 23] or spatial multiplexing by using two separate fibres [24] has been employed. Recently, combined polarization and frequency multiplexing in fibres has been demonstrated [25]. In laboratory free space QKD systems, spatial [26, 27] or polarization [28] multiplexing has been implemented. Using polarization multiplexing, signal and LO propagate in one spatial mode, such that no spatial interference stabilization is needed at the homodyne detector. This feature is particularly advantageous for atmospheric channels which are subject to spatial beam jitter.

In our continuous-variable QKD system, the following properties of a free space channel have to be considered:

Attenuation: In security analysis, channel losses are attributed to Eve who can split off a part of each signal state and perform measurements on it. At channel losses of more than 50%, Eve obtains more information about the signal than Bob. Although this problem can be circumvented by postselection [29] or reverse reconciliation [30], a low-loss channel is desirable since it allows for higher key rates. In clear weather conditions, atmospheric attenuation in the transmission windows (e.g. between 780 nm and 850 nm) is indeed low (<0.1 dB/km) [2].

Excess noise: In discrete-variable systems, the polarization angle between two different signals is large (e.g. $22.5°$ in the BB84 protocol), therefore any birefringent effects of the atmosphere are negligible [31]. In our continuous-variable system, on the other hand, the polarization tilt between different signals is very small. Although atmospheric depolarization effects are small [32, 33] they could cause significant excess noise (noise in excess of quantum noise resulting from the Heisenberg uncertainty principle). Excess noise is in principal assumed to stem from Eve's actions and therefore if it is too high security is compromised [34, 35, 36].

Spatial beam jitter: Atmospheric turbulence leads to fluctuations of the beam position at the receiver. Although this effect is not a fundamental limitation, it might lead to additional detection losses. The receiver's optical elements should therefore be designed to collect all the incoming light. This can be done by choosing appropriate aperture diameters and/or by actively stabilizing the beam direction. In situations where this is technically not feasible, protocols such as quantum filtering [37] can be employed.
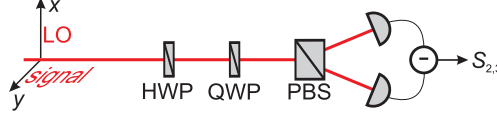
Figure 1. Stokes parameter measurement with half-wave plate (HWP), quarter-wave plate (QWP) and polarizing beam splitter (PBS). In our QKD experiment, the bright local oscillator is linearly polarized along the x-direction. Therefore, its only non-zero component is S_1. The y-polarized quantum signal is contained in the S_2 component. After appropriate adjustment of the wave plates, the homodyne signal appears in the difference between the currents of the two PIN photodiodes.

1.3. Homodyne detection of coherent polarization states

Polarization multiplexing of signal and LO [28, 38, 39] can be conveniently described in terms of Stokes operators [40]. These operators are the quantum analogue to the classical Stokes parameters [41] and read in our notation:

$$\hat{S}_0 = \hat{a}_x^\dagger \hat{a}_x + \hat{a}_y^\dagger \hat{a}_y \qquad \text{(total intensity)},$$
$$\hat{S}_1 = \hat{a}_x^\dagger \hat{a}_x - \hat{a}_y^\dagger \hat{a}_y \qquad (\leftrightarrow - \updownarrow),$$
$$\hat{S}_2 = \hat{a}_x^\dagger \hat{a}_y + \hat{a}_y^\dagger \hat{a}_x \qquad (\nearrow - \searrow),$$
$$\hat{S}_3 = i(\hat{a}_y^\dagger \hat{a}_x - \hat{a}_x^\dagger \hat{a}_y) \qquad (\circlearrowright - \circlearrowleft),$$

in terms of the creation and annihilation operators $\hat{a}^\dagger$ and $\hat{a}$. The arrows in brackets display the operational definitions of the Stokes parameters as intensity differences of polarization types.

In our experiment, the photon number in the x-mode is much larger than in the y-mode. In this situation, we can describe a Stokes measurement of $S_{2/3}$ as homodyne detection of $\hat{a}_y$ with the local oscillator in $\hat{a}_x$ (see figure 1). This configuration results in the uncertainty relation

$$\text{Var}(\hat{S}_2) \cdot \text{Var}(\hat{S}_3) \geq |\langle \hat{S}_1 \rangle|^2. \tag{1}$$

In the case of coherent states, the equality holds and the variances of $\hat{S}_2$ and $\hat{S}_3$ are equal. Excess noise leads to increased variances.

2. Experimental setup

We transfer the principle of our earlier laboratory experiments [28, 39] to a 100 m atmospheric channel on the flat roof of our institute's building (see figure 2). In this proof-of-principle experiment, we place Alice's and Bob's station on one optical table inside the building and send the beam out and back using a retro-reflector. The reflected beam propagates exactly parallel but spatially displaced with respect to the outgoing one. The retro-reflector is designed according to the cat's eye principle, with a mirror placed at the focal length of an achromatic lens. A corner cube retro-reflector is not suitable for our polarization encoding since it translates spatial beam jitter into polarization fluctuations [42]. Over the entire distance the beam propagates close to the roof surface. The temperature gradient of the roof and surrounding air thus provides us with appropriate real-world conditions for our investigations.
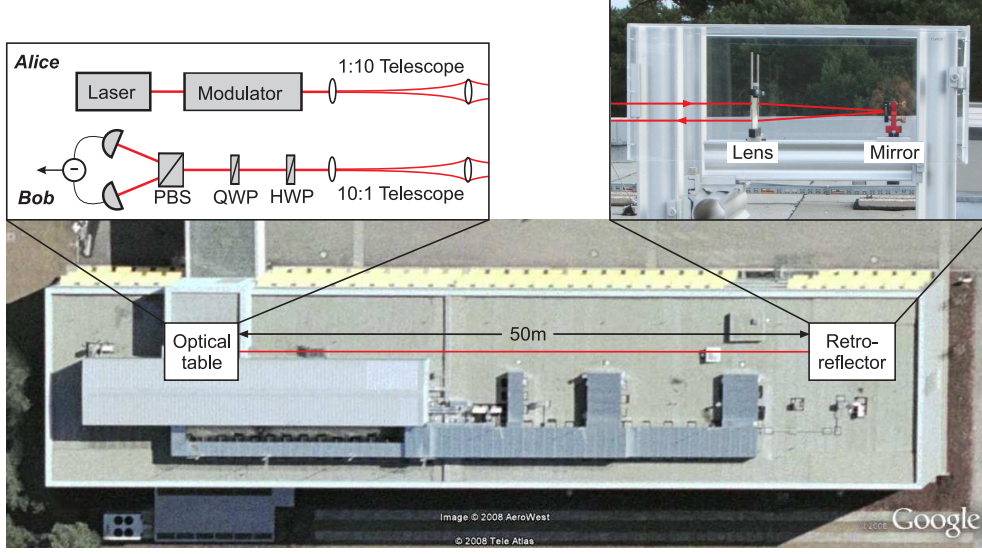
Figure 2. Experimental setup on the flat roof of our institute's building: Alice's laser emits a linearly polarized CW beam which later serves as a local oscillator for Bob's measurements. In terms of Stokes parameters, the local oscillator is S_1 polarized. Alice's magneto-optical modulator generates a weak signal in the S_2 component. The beam is expanded and sent to a retro-reflector at a distance of 50 m. The retro-reflector is designed according to the cat's eye principle with a mirror placed at the focal length of a lens. Bob performs a homodyne Stokes measurement on the reflected beam.

We use a grating-stabilized CW diode laser of wavelength 809 nm, which lies within one of the atmospheric transmission windows [2]§. After passing through a fibre mode-cleaner and a polarizing beam splitter, the laser beam is polarized along the x-direction. In other words, this light beam contains the x-polarized local oscillator in the S_1 component and vacuum in S_2 and S_3. By applying a current through the coil of the magneto-optical modulator (MOM) a magnetic field is generated. Via the Faraday effect, a magneto-optical crystal tilts the linear polarization of the light beam. This polarization tilt results in a weak S_2 component corresponding to an y-polarized signal in the same spatial mode as the local oscillator. The signal amplitude is taken out of the LO which, due to the weak modulation, remains essentially unaffected.

Using an arbitrary waveform generator, Alice randomly‖ generates one of two coherent states $|+\alpha\rangle$ or $|-\alpha\rangle$ (see figure 3). With this binary phase shift keying (BPSK) we use the smallest possible alphabet simplifying the analysis of statistical errors in a full security analysis. More complex alphabets along the S_2 axis could be easily generated by software modifications. For a modulation in the S_3 direction, an additional electro-optical modulator (EOM) could be incorporated into the setup [28]. An EOM could also generate states on a circle around the origin [44].

Before transmission through the free space channel, the signal/LO beam is

§ Another optical atmospheric window is located around 1550 nm. The larger beam diameters at the diffraction limit of these wavelengths, however, would demand larger optical elements.
‖ Here we use pseudo-random numbers for experimental simplicity. To generate real random numbers, Alice could split off a part of the LO and perform a homodyne measurement on the vacuum state [43].
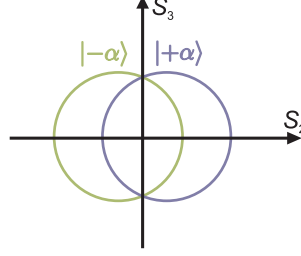
Figure 3. Contour plots of the two coherent states in our binary phase shift keying protocol. The amplitude α corresponds to the first moment of the Gaussian probability distributions. Due to the small amplitude the two states are nearly indistinguishable to Eve. By postselecting favourable measurement events, Bob gains an information advantage over Eve [29].

expanded by a 1/10 telescope such that its Rayleigh length corresponds to half the channel length. We thus obtain a collimated beam of diameter $\approx$1 cm whose waist we place onto the retro-reflector at a distance of 50 m. Bob's 10/1 telescope, in turn, reduces the beam diameter to $\approx$1 mm. A receiving lens of diameter 63 mm allows us to collect most of the spatially jittering beam without active stabilization.

In Bob's homodyne Stokes detection, the returning signal/LO beam is equally split into two parts by a Wollaston prism. Each beam is focused on a photodiode (Hamamatsu S3399) whose active area we chose to be larger than the beam size including beam jitter at the focal spot. The difference of the photocurrents from the two photodiodes is electronically amplified and processed by an analogue-to-digital converter. For an S_2 measurement, the detection basis is adjusted by a half-wave plate. Monitoring of the S_3 component [39] is not performed in this study, but will be implemented in future experiments. Alice's arbitrary waveform generator and Bob's analogue-to-digital converter are currently embedded in the same computer. Thus synchronization is easily achieved by an electric cable which transmits trigger signals from Alice to Bob.

3. Results

We commence this section with an investigation of the noise behaviour of our newly developed magneto-optical modulator. Next, we present measurements of atmospheric polarization noise. From the absence of significant excess noise in both cases we deduce that our system is suitable for QKD operation. Finally, we demonstrate the transmission of quantum states over the atmospheric channel and provide calculations of the achievable key rate.

3.1. Noise behaviour of the magneto-optic modulator

The bandwidth of our magneto-optical modulator (MOM) is limited by the inductance of the coil which generates the magnetic field. In the new version, the size of this coil has been decreased which enables us to operate the modulator at 1 MHz. When characterizing the MOM, we detect the modulated beam directly after modulation. We are therefore able to investigate the noise behaviour of the MOM separately from the free space channel.
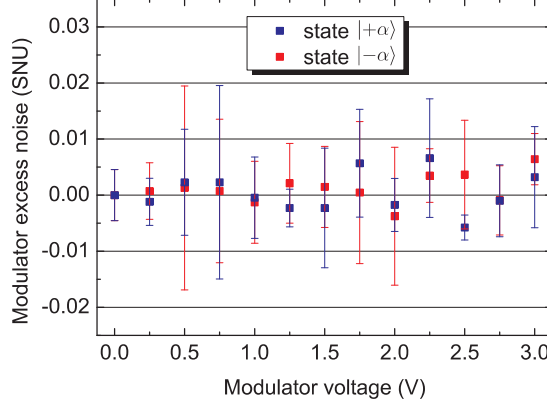
Figure 4. Excess noise (in shot noise units, SNU) introduced by the modulation of S_2. The modulation voltages are proportional to the amplitudes α of the coherent states (3.0 V corresponds to $\alpha = 0.21$). The noise has been determined separately for negative and positive modulations. Within the measuring accuracy we find that no significant excess noise is caused by modulation using the MOM.

A signal state is generated by applying a predefined positive or negative voltage to the MOM driver for 400 ns. After each signal pulse the modulation voltage is switched to zero for 600 ns to enable the modulator to return to its zero position. During this time, the signal is in the vacuum state. This vacuum reference is also needed for calibration since the polarization in the setup drifts slowly in time. We determine the vacuum level by calculating the mean value of 100 vacuum measurements neighbouring each signal pulse. This value is then subtracted from each signal measurement. At a constant vacuum level, an increased number of calibration pulses allows for a more precise calibration. In practice, however, this number is limited by slow polarization drifts as well as by laser excess noise at low frequencies.

We determine the excess noise of a signal state by comparing its variance to the variance of the vacuum state (shot noise). The variance of the vacuum state is normalized to unity. Figure 4 shows the excess noise introduced by the modulation for different signal amplitudes. We see that, within the measuring accuracy, the modulation does not generate a significant amount of excess noise.

3.2. Characterization of atmospheric polarization noise

We measure atmospheric polarization noise by recording the noise of an unmodulated beam on a spectrum analyzer. We calibrate to shot noise by comparing the spectra of $\mathrm{Var}(\hat{S}_2)$ before and after transmission through the free space channel. In both cases, the optical power at the detector is $0.5\,\mathrm{mW}\pm 3\%$. The measuring accuracy of the optical power is limited due to spatial beam jitter: the beam wanders across regions of slightly different quantum efficiency on the power meter. The measuring accuracy of the optical power S_0 translates to an inaccuracy in the noise measurement via the expression

$$|\langle \hat{S}_0 \rangle| \approx |\langle \hat{S}_1 \rangle| = \mathrm{Var}(\hat{S}_2) \tag{2}$$

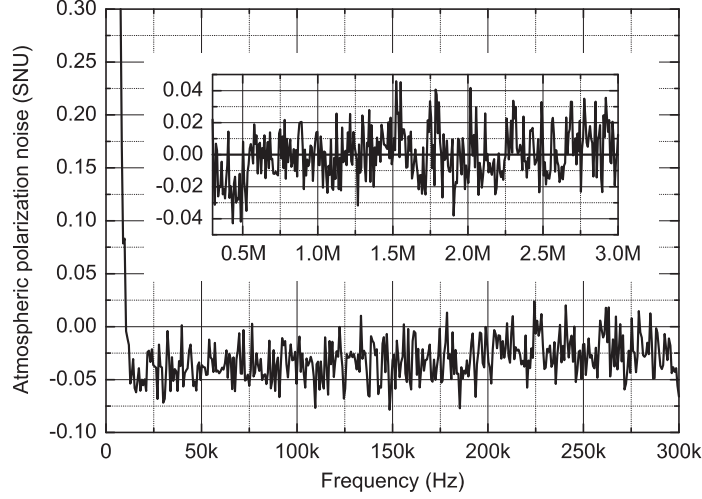which holds for a bright S_1 polarized beam at the quantum noise limit.

Figure 5. The determination of atmospheric polarization noise has been performed in two separate measurements from 0 to 300 kHz and from 300 kHz to 3 MHz (inset). Within the measuring accuracy of 3% we find no significant excess noise for frequencies above 10 kHz. We verified that background light at day or at night does not add noise to our measurements.

As displayed in figure 5, no significant excess noise is present above 10 kHz. The noise below 10 kHz amounts to less than 3 shot noise units which, due to the large magnification of the plot, result in an abrupt drop. This low-frequency noise stems at least partly from spatial beam jitter which causes the beam to wander across regions of slightly different quantum efficiency on the photodiodes. Our QKD signal at higher frequencies is not affected by the low-frequency noise. In a homodyne signal detection, however, the low-frequency deviations lead to an unbalance. In our measurements, this unbalance was typically around 1% and never exceeded 2%. A calculation following [45] reveals its impact on the quantum states: Firstly, since we adjust our laser to operate at the shot noise limit, the unbalance results in excess noise of less than 1% which is lower than the detector's electronic noise. Secondly, the detection efficiency is varying by less than 1%. This effect might give an eavesdropper an, albeit small, possibility to gain information [46] and thus should be considered in future security analyses. As already mentioned in section 3.1, we have to choose the number of vacuum calibration pulses such that their level does not change due to low-frequency deviations.

3.3. Quantum signal measurements and estimation of secure key rate

To obtain the optimal key rate, the signal amplitude α has to be adapted to the losses in the QKD system. We perform an optimization of α assuming postselection [29] and realistic two-way error correction procedures (CASCADE [47]). Intuitively, the existence of an optimum can be explained as follows: For too small amplitudes, Bob obtains low information due to the high error rate. In the case of too large amplitudes, on the other hand, Eve's information is also large. To gain an information advantage, Bob must apply a high postselection threshold thus discarding many measurements.

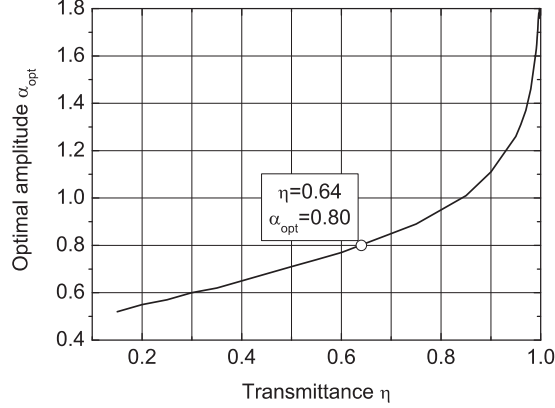Assuming a noiseless channel, the expected key rate G is equal to the difference

Figure 6. Calculation of the optimal signal amplitude α_{opt} as a function of the transmittance η. For the overall transmittance $\eta = 0.64$ in our experiment, we find the optimal amplitude $\alpha_{\mathrm{opt}} = 0.80$.

between Bob's and Eve's information [48]:

$$G = \int_0^\infty \left(1 - f[e]H[e] - S[\hat{\rho}_E]\right) p(\beta)\mathrm{d}\beta, \tag{3}$$

where $f[e]$ is the efficiency of CASCADE, e is Bob's error rate, H is the standard Shannon entropy, $p(\beta)$ is the probability of measuring the value β, and $S[\hat{\rho}_E]$ is the von Neumann entropy of Eve's density matrix $\hat{\rho}_E$. We apply postselection by accepting only positive contributions to the integral in (3). The exact value of the optimal amplitude α_{opt} is calculated numerically by maximizing the key rate for a given transmittance η (see figure 6). The higher the transmittance, the less information can be potentially obtained by Eve, and the higher the optimal amplitude.

The transmittance of our 100 m free space channel is $\eta_{\mathrm{ch}} = 0.77$, with losses originating mainly from the retro-reflector. In a conservative calculation we also attribute detection losses $(1 - \eta_{\mathrm{det}}) = 0.17$ to Eve. For the overall transmittance $\eta = \eta_{\mathrm{ch}} \cdot \eta_{\mathrm{det}} = 0.64$, the optimal amplitude is $\alpha_{\mathrm{opt}} = 0.80$.

At the moment, technical constraints prevent us from reaching the optimal amplitude at a pulse rate of 1 MHz. For this reason, we choose a pulse rate of 100 kHz in the following. Measurement results for the amplitude $\alpha_{\mathrm{opt}} = 0.80$ are shown in figure 7 where we plot the error rates of measurements with and without free space channel. For better comparison, we adjust the detected optical power to be equal in both cases: any attenuation in the channel is effectively factored out. Thus the measured quantum states differ only with respect to their excess noise. Excess noise from the free space channel would increase the error rate. Within the measuring accuracy, however, we find no increased error rate which confirms that atmospheric excess noise is insignificant.

The optimal postselection threshold β_0^{opt} is found by solving the equation $I_{\mathrm{AB}} = I_{\mathrm{AE}}$, where I_{AB} is the mutual information between Alice and Bob, and I_{AE} between Alice and Eve. This means Bob accepts only those signals which positively contribute to the total key. The key rate G as a function of the postselection threshold β_0 is shown in figure 8. We can see that the postselection threshold has to be set correctly, otherwise the key rate is reduced. At the optimal postselection threshold
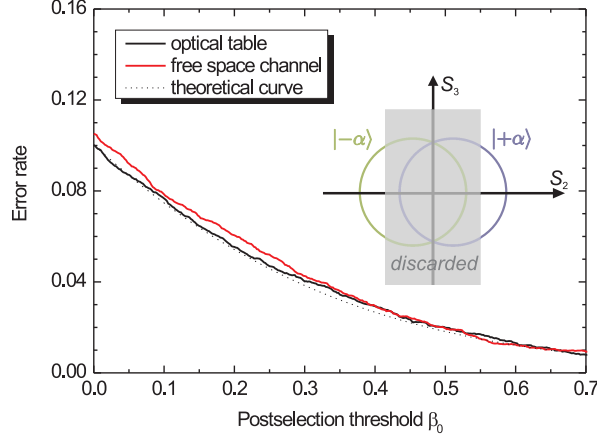
Figure 7. Error rates after postselection for coherent states with amplitude $\alpha = 0.80$. Increasing the postselection threshold (see inset) discards more ambiguous states and thus reduces the error rate. The measured error rates with and without the free space channel are equal within the measuring accuracy. This indicates that the quantum states are not affected by real atmospheric conditions. The measurements follow the theoretical curve $\frac{\mathrm{erfc}[\sqrt{2}(\beta_0 + \sqrt{\eta}\alpha)]}{2P(\beta_0, \sqrt{\eta}\alpha)}$, where $P(\beta_0, \sqrt{\eta}\alpha)$ is the acceptance probability of the postselection [49].
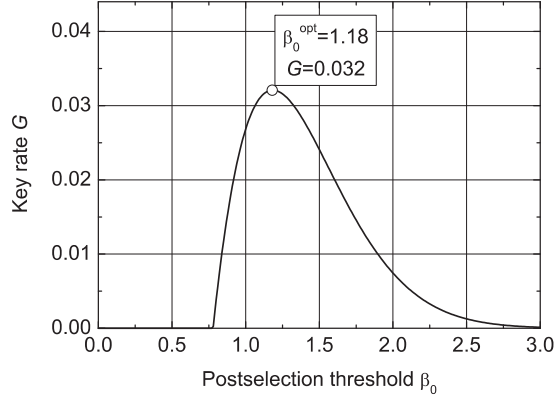

Figure 8. Calculation of the key rate G for the transmittance $\eta = 0.64$ and the signal amplitude $\alpha = 0.80$. At the optimal postselection threshold $\beta_0^{\mathrm{opt}} = 1.18$, the key rate is $G = 0.032$.

$\beta_0^{\mathrm{opt}} = 1.18$, the key rate would be $3.2\,\mathrm{kbit/s}$ at a pulse rate of $100\,\mathrm{kHz}$.

4. Conclusions and Outlook

We have demonstrated the low-noise transmission of coherent polarization states over a real-world atmospheric channel. Our results indicate that our system is suitable

for establishing a QKD link in urban environments in daylight. To the best of our knowledge, this experiment is the first continuous-variable quantum communication under real atmospheric conditions.

In future work, we want to extend our system to a point-to-point link in an urban environment. To synchronize Alice's and Bob's stations, we plan to interrupt the LO (and therefore also the signal) in regular time intervals. Switching on the LO will mark the beginning of a signal frame each containing about 1000 signal states. To avoid optical losses, we will choose the telescopes' diameter larger than the beam size including beam wander. Drifts in the telescopes' pointing direction could be compensated by an active pointing control [50] with the LO as control signal.

Furthermore, we intend to increase the pulse modulation rate above 10 MHz. For this frequency range, signal generators as well as digital-to-analogue converters are commercially available and detectors with low electronic noise have been built in our laboratory. Thus the limitation in pulse rate is only due to our magneto-optical modulator. However, the bandwidth of a magneto-optical modulator can in principle reach the GHz range (see [51] and references therein). Electro-optical modulators, on the other hand, are commercially available and could be used in our experiment as well [28].

Another interesting field of study is analyzing attacks on the implementation of our system. An eavesdropper could, for example, gain advantage by manipulating the local oscillator [52] or by artificially tilting the beam to modify the efficiency of Bob's detectors [46].

Acknowledgments

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2008 arXiv:0802.4155v2 [quant-ph]
[3] Majumdar A K and Ricklin J C (eds) 2008 *Free-Space Laser Communications* (*Optical and Fiber Communications Reports* vol 2) (Berlin: Springer)
[4] Jacobs B C and Franson J D 1996 *Opt. Lett.* **21** 1854
[5] Rarity J G, Tapster P R and Gorman P M 2001 *J. Mod. Optics* **48** 1887
[6] Kurtsiefer C, Zarda P, Halder M, Weinfurter H, Gorman P M, Tapster P R and Rarity J G 2002 *Nature* **419** 450
[7] Hughes R J, Nordholt J E, Derkacs D and Peterson C G 2002 *New J. Phys.* **4** 43
[8] Bienfang J C, Gross A J, Mink A, Hershman B J, Nakassis A, Tang X, Lu R, Su D H, Clark C W and Williams C J 2004 *Opt. Express* **12** 2011
[9] Schmitt-Manderbach T *et al.* 2007 *Phys. Rev. Lett.* **98** 010504
[10] Peng C Z *et al.* 2005 *Phys. Rev. Lett.* **94** 150501
[11] Ursin R *et al.* 2007 *Nat. Phys.* **3** 481
[12] Ling A, Peloso M P, Marcikic I, Scarani V, Lamas-Linares A and Kurtsiefer C 2008 *Phys. Rev. A* **78** 020301(R)
[13] Erven C, Couteau C, Laflamme R and Weihs G 2008 *Opt. Express* **16** 16840
[14] Villoresi P *et al.* 2008 *New J. Phys.* **10** 033038
[15] Perdigues Armengol J M *et al.* 2008 *Acta Astronaut.* **63** 165
[16] Miao E L, Han Z F, Gong S S, Zhang T, Diao D S and Guo G C 2005 *New J. Phys.* **7** 215
[17] Shan X, Sun X, Luo J, Tan Z and Zhan M 2006 *Appl. Phys. Lett.* **89** 191121

[18] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India) p 175
[19] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[20] Ralph T C 1999 *Phys. Rev. A* **61** 010303(R)
[21] Lodewyck J *et al.* 2007 *Phys. Rev. A* **76** 042305
[22] Legré M, Zbinden H and Gisin N 2006 *Quantum Inf. Comput.* **6** 326
[23] Wittmann C, Fürst J, Wiechers C, Elser D, Sych D and Leuchs G *in preparation*
[24] Lodewyck J, Debuisschert T, Tualle-Brouri R and Grangier P 2005 *Phys. Rev. A* **72** 050303(R)
[25] Qi B, Huang L L, Qian L and Lo H K 2007 *Phys. Rev. A* **76** 052323
[26] Hirano T, Yamanaka H, Ashikaga M, Konishi T and Namiki R 2003 *Phys. Rev. A* **68** 042331
[27] Lance A M, Symul T, Sharma V, Weedbrook C, Ralph T C and Lam P K 2005 *Phys. Rev. Lett.* **95** 180503
[28] Lorenz S, Korolkova N and Leuchs G 2004 *Appl. Phys. B* **79** 273
[29] Silberhorn C, Ralph T C, Lütkenhaus N and Leuchs G 2002 *Phys. Rev. Lett.* **89** 167901
[30] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238
[31] Toyoshima M, Takayama Y, Klaus W, Kunimori H, Fujiwara M and Sasaki M 2008 *Acta Astronaut.* **63** 179
[32] Boyer G R and Prade B S 1976 *Surf. Sci.* **56** 449
[33] Crosignani B, Di Porto P and Clifford S F 1988 *Appl. Optics* **27** 2183
[34] Rigas J, Gühne O and Lütkenhaus N 2006 *Phys. Rev. A* **73** 012341
[35] Heid M and Lütkenhaus N 2007 *Phys. Rev. A* **76** 022313
[36] Zhao Y B, Heid M, Rigas J and Lütkenhaus N 2009 *Phys. Rev. A* **79** 012307
[37] Wittmann C, Elser D, Andersen U L, Filip R, Marek P and Leuchs G 2008 *Phys. Rev. A* **78** 032315
[38] Vidiella-Barranco A and Borelli L F M 2006 *Int. J. Mod. Phys. B* **20** 1287
[39] Lorenz S, Rigas J, Heid M, Andersen U L, Lütkenhaus N and Leuchs G 2006 *Phys. Rev. A* **74** 042326
[40] Korolkova N, Leuchs G, Loudon R, Ralph T C and Silberhorn C 2002 *Phys. Rev. A* **65** 052306
[41] Stokes G G 1852 *Trans. Cambridge Philos. Soc.* **9** 399
[42] Liu J and Azzam R M A 1997 *Appl. Opt.* **36** 1553
[43] Trifonov A and Vig H 2007 U. S. Patent 7284024
[44] Sych D and Leuchs G 2009 arXiv:0902.1895v1 [quant-ph]
[45] Lorenz S 2005 *Experimentelle Quantenkryptographie mit kontinuierlichen Variablen* Phd thesis Institute of Optics, Information and Photonics, University of Erlangen-Nuremberg, URL `http://www.opus.ub.uni-erlangen.de/opus/volltexte/2005/278/`
[46] Fung C H F, Tamaki K, Qi B, Lo H K and Ma X 2009 *Quantum Inf. Comput.* **9** 0131
[47] Brassard G and Salvail L 1994 *Advances in Cryptology — EUROCRYPT '93* (*Lecture notes in Computer Science* vol 765) ed Helleseth T (Berlin: Springer) p 410
[48] Heid M and Lütkenhaus N 2006 *Phys. Rev. A* **73** 052316
[49] Namiki R and Hirano T 2003 *Phys. Rev. A* **67** 022308
[50] Weier H 2003 *Experimental Quantum Cryptography* Diploma thesis, Physics Department, Technical University of Munich
URL `http://scotty.quantum.physik.uni-muenchen.de/people/weier.html`
[51] Irvine S E and Elezzabi A Y 2003 *J. Phys. D* **36** 2218
[52] Häseler H, Moroder T and Lütkenhaus N 2008 *Phys. Rev. A* **77** 032303